

A NOTE ON DIAGONAL AND HERMITIAN SURFACES

IAN BLAKE, V. KUMAR MURTY, AND HAMID USEFI

ABSTRACT. Aspects of the properties, enumeration and construction of points on diagonal and Hermitian surfaces have been considered extensively in the literature and are further considered here. The zeta function of diagonal surfaces is given as a direct result of the work of Wolfmann. Recursive construction techniques for the set of rational points of Hermitian surfaces are of interest. The relationship of these techniques here to the construction of codes on surfaces is briefly noted.

1. INTRODUCTION

The enumeration of points on hypersurfaces over finite fields has been a problem of interest in the study of algebraic geometry, culminating in the celebrated conjectures and theorems of Weil and Deligne. The case of surfaces defined by diagonal equations has been of particular interest and the work of Wolfmann [25] gives expressions for these for the cases of interest in this work. These expressions are examined further here with a view to understanding their properties better.

The next Section 2 considers the case of surfaces from diagonal equations and, in particular, the important results of Wolfmann [25] on the enumeration of diagonal surfaces. The properties of functions introduced by Wolfmann are explored. Section 3 gives a brief review of aspects of algebraic curves and hypersurfaces over a finite field and their zeta functions. In particular, the zeta function of diagonal surfaces is seen to follow as a direct consequence of this work.

One of the motivations of this work was to apply the recursive construction of the points on Hermitian surfaces and their properties to derive results on the minimum distance of codes obtained from Hermitian surfaces, a problem that has attracted considerable attention. While this approach has so far been unsuccessful, the problem is discussed in Section 4.

2. ENUMERATION OF DIAGONAL SURFACES

While much of the remainder of the paper will consider projective surfaces over the finite field \mathbb{F}_q , this section will consider the affine case and the results of Wolfmann [25]. So far as possible the notation of Wolfmann will be used although there will be important differences to accommodate our interests in the projective cases in later sections.

Date: November 14, 2014.

The research of the first and second author are supported by NSERC. The research of the third author is supported by NSERC and the Research & Development Corporation of Newfoundland and Labrador.

Denote by $N_{0,k,s}$ the number of solutions over \mathbb{F}_{q^k} of the equation

$$(1) \quad x_1^d + x_2^d + \cdots + x_s^d = 0$$

where $q = p^{2r}$ and $d \mid p^r + 1$. The parameter d will be fixed throughout. Define the function $B(d, s)$ as:

$$(2) \quad B(d, s) = \frac{1}{d} ((d-1)^s + (-1)^s (d-1)).$$

The following result of Wolfmann is central to this work.

Theorem 2.1 ([25], Corollary 4). *Let p be a prime number, $q = p^{2r}$, and \mathbb{F}_{q^k} the finite field of order q^k . The number of solutions to the equation*

$$x_1^d + x_2^d + \cdots + x_s^d = b, \quad b \in \mathbb{F}_{q^k}$$

for $d \mid p^r + 1$, $nd = q^k - 1$ and $s \geq 2$ is as follows:

- (1) *If $b = 0$ we have $N_{0,k,s} := q^{k(s-1)} + \eta^s q^{k(s/2-1)} (q^k - 1) B(d, s)$.*
- (2) *If $b \neq 0$ and $b^n = 1$ then $N_{1,k,s} := q^{k(s-1)} + \eta^{s+1} q^{k(s/2-1)} [(d-1)^s q^{k/2} - (q^{k/2} + \eta) B(d, s)]$.*
- (3) *If $b \neq 0$ and $b^n \neq 1$ then $N_{2,k,s} := q^{k(s-1)} + \eta^{s+1} q^{k(s/2-1)} [(-1)^s q^{k/2} - (q^{k/2} + \eta) B(d, s)]$,*

where $\eta = (-1)^{k+1}$ and $B(d, s)$ is as in Equation (2).

Let α be a primitive root of \mathbb{F}_{q^k} . Notice that the equation $b^n = 1$ has n solutions in \mathbb{F}_{q^k} if and only if $b = \alpha^{jd}$ for some integer j . Define the n -th roots of unity as $U_n = \{\alpha^{jd}, j = 0, 1, \dots, (n-1)\}$ and notice that the equation $x^d = a$ has solutions if and only if $a \in U_n$. If α^i is a solution of this equation, the other solutions are $\alpha^{i+\ell n}$ for $\ell = 0, 1, \dots, (d-1)$.

Also notice that $-1 \in U_n$. This is argued as follows. If p is even (characteristic 2) then $-1 = +1$ and is in U_n . If p is odd then $n = (q^k - 1)/d = (p^{2rk} - 1)/d = (p^{rk} - 1)(p^{rk} + 1)/d$ and since by assumption $d \mid (p^r + 1)$ it divides either the first or second factor. As both factors are even, so is n . Thus if $a \in U_n$ then so is $-a$.

Many relationships among the quantities mentioned in the above Theorem can be formulated. Three of these are noted below as of sufficient interest to prove.

Lemma 2.2. *With the notation of Theorem (2.1), we have*

$$N_{0,k,s+1} = N_{0,k,s} + (q^k - 1) N_{1,k,s}.$$

Proof: The Lemma is a reflection of the fact that a solution to the Equations (1) with s variables to one with $(s+1)$ variables can be developed in two ways, the first being by adding a zero for the $(s+1)$ -st variable to a solution to an s variable one. The other considers the situation where a solution $\mathbf{y} = (y_1, y_2, \dots, y_s)$ satisfies

$$y_1^d + y_2^d + \cdots + y_s^d = b \in U_n.$$

The equation $x^d = b \in U_n$ has d solutions which can be added as the $(s+1)$ -st coordinate to the solution \mathbf{y} . There are such n such values of b giving rise to nd such solutions and the second term of the Lemma as $nd = (q^k - 1)$.

The equations of the Lemma can be expressed:

$$\begin{aligned} N_{0,k,s+1} &= q^{k(s)} + \eta^{s+1} q^{k((s+1)/2-1)} (q^k - 1) B(d, s+1) \\ &= q^{k(s-1)} + \eta^s q^{k(s/2-1)} (q^k - 1) B(d, s) + \\ &\quad (q^k - 1) (q^{k(s-1)} + \eta^{s+1} q^{k(s/2-1)} [(d-1)^s q^{k/2} - (q^{k/2} + \eta) B(d, s)]) \end{aligned}$$

Verification of this equation is straightforward. \square

Lemma 2.3. *With the notation of Theorem (2.1), we have $q^{ks} = N_{0,k,s} + nN_{1,k,s} + (q^k - 1 - n)N_{2,k,s}$.*

Proof: The Lemma reflects the fact that as the variables $x_i, i = 1, 2, \dots, s$ range over all values of \mathbb{F}_{q^k} , the sum $\sum_i x_i^d$ takes on values either 0, $b \in U_n$ or $b \notin U_n$. The direct proof, omitted here, involves verifying the equation:

$$\begin{aligned} q^{ks} &= q^{k(s-1)} + \eta^s q^{k(s/2-1)} (q^k - 1) B(d, s) \\ &\quad + n \cdot (q^{k(s-1)} + \eta^{s+1} q^{k(s/2-1)} [(d-1)^s q^{k/2} - (q^{k/2} + \eta) B(d, s)]) \\ &\quad + (q^k - n - 1) \cdot (q^{k(s-1)} + \eta^{s+1} q^{k(s/2-1)} [(-1)^s q^{k/2} - (q^{k/2} + \eta) B(d, s)]). \end{aligned}$$

\square

Lemma 2.4. *Let i be an integer in the range $1 \leq i \leq s-1$. Then, with the notation of Theorem (2.1), we have*

$$N_{0,k,s} = N_{0,k,i} N_{0,k,s-i} + n N_{1,k,i} N_{1,k,s-i} + (q^k - 1 - n) N_{2,k,i} N_{2,k,s-i}.$$

Proof: The relation enumerates the solutions to the equation

$$x_1^d + x_2^d + \dots + x_i^d = a.$$

If $a = 0$, any such solution can be combined with a solution to $x_{i+1}^d + \dots + x_s^d = 0$ to yield the first term. Since if $a \in U_n$ then so is $-a$ and there are n such values which gives the second term and similarly for the third term.

The formal verification involves substituting the expressions from Theorem (2.1) and is omitted. \square

Finally it is interesting to note that if, for a given value of d , the terms $N_{0,k,s}$ are known for all k and s , then by applying Lemmas 2.2 and 2.3, they determine all other terms, $N_{1,k,s}$ and $N_{2,k,s}$. Thus the zero solutions determine uniquely all nonzero solutions.

3. THE ZETA FUNCTION OF A DIAGONAL SURFACE

For the remainder of the work the projective case will be of interest and the affine results of the previous section will be translated to the projective case. The projective space of dimension s over \mathbb{F}_{q^k} , denoted by $\mathbb{P}_{q^k}^s$, is the set of $(s + 1)$ -tuples, or points, over the finite field \mathbb{F}_{q^k} with scalar multiples identified. Thus

$$(3) \quad \mathbb{P}_{q^k}^s = \{(a_0, a_1, \dots, a_s), a_i \in \mathbb{F}_{q^k}\}, \quad |\mathbb{P}_{q^k}^s| = (q^{k(s+1)} - 1)/(q^k - 1) = \pi_{q^k, s}.$$

Where needed, the representative of an equivalence class will have the first nonzero element in the $(s + 1)$ tuple is unity. When q^k is understood, we write $\pi_{q^k, s} = \pi_s$.

For the homogeneous polynomial $f(x_0, x_1, \dots, x_s)$ over \mathbb{F}_{q^k} define the projective variety

$$X_f(\mathbb{F}_{q^k}) = \{(x_0, x_1, \dots, x_s) \in \mathbb{P}_{q^k}^s \mid f(x_0, x_1, \dots, x_s) = 0\}.$$

The variety is referred to as a hypersurface when defined by a single polynomial as above. It is also referred to as the zero set or *algebraic set* of f . More general varieties over \mathbb{F}_{q^k} defined by sets of polynomials, will simply be denoted $X(\mathbb{F}_{q^k})$. The hypersurface is called *nondegenerate* ([16]) if it is not contained in a linear subspace of $\mathbb{P}_{q^k}^s$, *smooth* if it contains no singularities (points where the function derivatives vanish simultaneously) and irreducible if it is not the union of smaller algebraic sets. Many of the results considered have parallels in the associated affine case.

If the homogeneous polynomial f with $(s+1)$ variables is of degree d the variety is referred to as having dimension s and degree d . The polynomials of interest here, as in the previous section, are the diagonal ones:

$$(4) \quad x_0^d + x_1^d + \dots + x_s^d = f(x_0, x_1, \dots, x_s)$$

The corresponding surfaces will be referred to as *diagonal*. The base field will be taken as \mathbb{F}_q , $q = p^{2r}$ for some prime p . When $d = p^r + 1$ in the above equation, the variety over \mathbb{F}_q will be referred to as *Hermitian*. When viewing this diagonal equation over extensions of \mathbb{F}_q it would cease to be Hermitian.

The cardinality of projective varieties has been of great interest in the literature. The case of affine varieties has been considered in the previous section. To translate them to the projective case, denote the number of projective points of the variety defined by the diagonal polynomial over \mathbb{F}_{q^k} of Equation (4) as $N'_{k,s}$ and note that

$$(5) \quad N'_{k,s} = \frac{(N_{0,k,s+1} - 1)}{(q^k - 1)} = |X_f(\mathbb{F}_{q^k})|$$

where primes will be used to denote the projective case and where f is the diagonal polynomial of Equation (4).

Much effort has been spent on determining bounds on the number of points on curves and surfaces. An early result of Weil (following a conjecture of Hasse) for curves of genus g is that

$$|N - (1 + q)| \leq 2gq^{1/2},$$

a result that was later improved by Serre to

$$|N - (1 + q)| \leq g \lfloor 2q^{1/2} \rfloor.$$

For the case of higher dimensional surfaces the generalized Weil-Deligne bound for a smooth nondegenerate hypersurface $X(\mathbb{F}_q)$, of dimension s and degree d is given by [16, 22, 25]:

$$(6) \quad |X_f(\mathbb{F}_q) - \pi_{q,s-1}| \leq B(d, s+1)q^{(s-1)/2},$$

where the function $B(d, s)$, given in Equation (2), will be useful in much of the sequel.

The Tsfasman-Serre-Sorensen bound [10, 21] for the same quantity is given by:

$$(7) \quad |X_f(\mathbb{F}_q)| \leq dq^{s-1} + \pi_{q,s-2},$$

a relationship that can be used to establish the minimum distance of certain projective geometry codes, as discussed later. The bound of this last equation is achieved only if the zero set of the defining polynomial consists of a union of d hyperspaces with a common hyperspace of co-dimension 2 [8, 18].

The zeta function of a curve or surface codifies the sizes of the variety when viewed over extension fields. Specifically let $X(\mathbb{F}_q)$ denote a variety of dimension s and degree d defined over the finite field \mathbb{F}_q and $X(\mathbb{F}_{q^k})$ for the same variety viewed over the extension field \mathbb{F}_{q^k} . Let $N'_{k,s}$ denote the number of projective solutions to this equation over \mathbb{F}_{q^k} and define the zeta function for $X(\mathbb{F}_q)$ as

$$Z_s(t) = \exp \left(\sum_{k=1}^{\infty} N'_{k,s} t^k / k \right),$$

where the dependence on the variety is understood.

The following information on zeta functions is well known eg [11, 15, 22, 27]. It is a rational function that can be expressed as

$$Z_s(t) = \frac{P_1(t)P_3(t) \dots P_{2m-1}(t)}{P_0(t)P_2(t) \dots P_{2m}(t)}$$

where the polynomials have integer coefficients and

$$P_i(t) = \prod_{j=1}^{b_i} (1 - \omega_{ij}t), \quad 1 \leq i \leq 2m-1$$

where b_i is a Betti number, related to the topology of the variety, the ω_{ij} are algebraic integers and $|\omega_{ij}| = q^{1/2}$ and $P_0(t) = 1-t$, $P_{2m}(t) = 1-q^m t$. The polynomials have many properties and we refer the reader to [11, 15, 27].

In the case the variety is smooth the zeta function can be refined to [14, 15, 20]:

Theorem 3.1. *Let $X_f(\mathbb{F}_q)$ be a smooth irreducible hypersurface over \mathbb{F}_q in \mathbb{P}_q^s of degree d and dimension s . Then*

$$Z_s(t) = \begin{cases} \frac{P(t)}{\prod_{i=0}^{s-1} (1 - q^i t)}, & s \text{ even} \\ \frac{1}{P(t) \prod_{i=0}^{s-1} (1 - q^i t)}, & s \text{ odd} \end{cases}$$

where $P(t) = \prod_{i=1}^{B(d,s+1)} (1 - \alpha_i t)$ and $B(d, s+1)$ is as in Equation (2). $P(t)$ has integer coefficients and $|\alpha_i| = q^{(s-1)/2}$.

The results of Wolfmann in the previous section can be applied to obtain the zeta functions of diagonal surfaces by noting that in the projective case

$$N'_{k,s} = \frac{q^{ks} - 1}{q^k - 1} + \eta^{s+1} q^{k(s-1)/2} B(d, s+1), \quad \eta = (-1)^{k+1}.$$

and hence

$$\begin{aligned} \ln(Z_s(t)) &= \sum_{k=1}^{\infty} N'_{k,s} t^k / k \\ &= \sum_{k=1}^{\infty} \{1 + q^k + \dots + q^{k(s-1)} + \eta^{s+1} B(d, s+1) q^{k(s-1)/2}\} t^k / k \end{aligned}$$

If $(s+1)$ is even then $\eta^{s+1} = 1$ and

$$\ln(Z_s(t)) = \sum_{j=0}^{s-1} \{-\ln(1 - q^j t)\} - B(d, s+1) \ln(1 - q^{(s-1)/2} t)$$

while if $(s+1)$ is odd then $\eta^{s+1} = (-1)^{(k+1)(s+1)} = (-1)^{k+1}$ and

$$\ln(Z_s(t)) = \sum_{j=0}^{s-1} \{-\ln(1 - q^j t)\} + B(d, s+1) \ln(1 + q^{(s-1)/2} t).$$

Thus the zeta function for diagonal surfaces is given by:

Theorem 3.2.

$$Z_s(t) = \begin{cases} (1 + q^{(s-1)/2} t)^{B(d,s+1)} / \prod_{i=0}^{s-1} (1 - q^i t), & s \text{ even} \\ 1 / (1 - q^{(s-1)/2} t)^{B(d,s+1)} \prod_{i=0}^{s-1} (1 - q^i t), & s \text{ odd}. \end{cases}$$

The theorem makes explicit the more general Theorem (3.1) for the case that $q = p^{2r}$ and $d \mid (p^r + 1)$.

The zeta function for the case $d = p^r + 1 = q^{1/2} + 1$ i.e. the curve over the base field is Hermitian, and is given by substituting these parameters in the above expression.

The expressions of the Lemmas (2.2) to Lemma (2.4) are sufficiently complex that it is an interesting exercise to briefly verify them with the expressions of Theorem (2.1). Only Lemma (2.2) is considered - Lemma (2.3) can be dealt with in the same manner. Subtracting 1 from each side of the equation in Lemma (2.2) and dividing by $(q^k - 1)$ gives for the projective variety of dimension s ,

$$N'_{k,s} = N'_{k,(s-1)} + N_{1,k,s}$$

and it follows immediately that

$$Z_s(t) = Z_{s-1}(t) \cdot F(s, t)$$

where

$$F(s, t) = \exp \left(\sum_{k=1}^{\infty} N_{1,k,s} t^k / k \right)$$

and the zeta functions for dimensions s and $(s-1)$ are given in the previous theorem and:

$$(8) \quad \frac{Z_s(t)}{Z_{s-1}(t)} = \begin{cases} (1 + q^{(s-1)/2}t)^{B(d,s+1)} \cdot (1 - q^{(s-2)/2}t)^{B(d,s)} / (1 - q^{(s-1)}t), & s \text{ even} \\ 1/(1 - q^{(s-1)}t) \cdot (1 - q^{(s-1)/2}t)^{B(d,s+1)} \cdot (1 + q^{(s-2)/2}t)^{B(d,s)}, & s \text{ odd} \end{cases}$$

To show the right hand side of this equation is $F(s, t)$ notice first that

$$B(d, s+1) + B(d, s) = (d-1)^s.$$

and recall $\eta = (-1)^{k+1}$. Then:

$$\begin{aligned} F(s, t) &= \sum_{k=1}^{\infty} N_{1,k,s} t^k / k \\ &= \sum_{k=1}^{\infty} \{ q^{k(s-1)} + \eta^{s+1} q^{k(s-2)/2} [(d-1)^s q^{k/2} - (\eta + q^{k/2}) B(d, s)] \} t^k / k \\ &= \sum_{k=1}^{\infty} \{ q^{k(s-1)} + \eta^{s+1} q^{k(s-2)/2} [q^{k/2} B(d, s+1) - \eta B(d, s)] \} t^k / k \end{aligned}$$

The three terms of the sum are evaluated as follows:

$$\begin{aligned} \sum_{k=1}^{\infty} q^{k(s-1)} t^k / k &= \sum_{k=1}^{\infty} (q^{s-1} t)^k / k = -\ln(1 - q^{s-1} t) \\ \sum_{k=1}^{\infty} (-1)^{(s+1)(k+1)} q^{k(s-1)/2} B(d, s+1) t^k / k &= (-1)^{s+1} B(d, s+1) \sum_{k=1}^{\infty} [(-1)^{s+1} q^{(s-1)/2} t]^k / k \\ &= \begin{cases} B(d, s+1) [-\ln(1 - q^{(s-1)/2} t)], & s \text{ odd} \\ B(d, s+1) [\ln(1 + q^{(s-1)/2} t)], & s \text{ even} \end{cases} \end{aligned}$$

and

$$\begin{aligned} -\sum_{k=1}^{\infty} \eta^{s+2} q^{k(s-2)/2} B(d, s) t^k / k &= -B(d, s) \sum_{k=1}^{\infty} (-1)^{s(k+1)} (q^{(s-2)/2} t)^k / k \\ &= \begin{cases} -B(d, s) \ln(1 + q^{(s-2)/2} t), & s \text{ odd} \\ +B(d, s) \ln(1 - q^{(s-2)/2} t), & s \text{ even} \end{cases} \end{aligned}$$

Putting the three terms together gives:

$$F(s, t) = \begin{cases} 1/[(1 - q^{(s-1)}t)(1 - q^{(s-1)/2}t)^{B(d, s+1)}(1 - q^{(s-2)/2}t)], & s \text{ odd} \\ [(1 + q^{(s-1)/2}t)^{B(d, s+1)}(1 - q^{(s-2)/2}t)^{B(d, s)}]/(1 - q^{(s-1)}t), & s \text{ even} \end{cases}$$

Using the form of the zeta functions $Z_s(t)$ and $Z_{s-1}(t)$ of Theorem (3.2) shows that this is precisely the $Z_s(t)/Z_{s-1}(t)$ given in Equation (8).

Recall that the assumption that $d \mid p^r + 1$ is a requirement of the results of [25] that is not present in the statement of Theorem(3.1).

4. STRUCTURE OF HERMITIAN SOLUTIONS SET AND CODING

Results of the previous section are interpreted here for the case of Hermitian surfaces which we restate as the set of projective solutions of the equation

$$(9) \quad x_0^{p^r+1} + x_1^{p^r+1} + \dots + x_s^{p^r+1} = 0,$$

over the finite field \mathbb{F}_q where $q = p^{2r}$, where p, q, r are fixed for this section. It will be referred to as the s -th dimensional Hermitian equation. The enumeration of the size of these varieties is well known [3, 4]:

$$(10) \quad (p^{r(s-1)} - (-1)^{(s+1)})(p^{rs} - (-1)^s)/(q - 1) = N'_{1,s}.$$

It is easy to establish the equality of this with

$$N'_{1,s} = \frac{(N_{0,1,s+1} - 1)}{(q - 1)} = h_s = q^{s-1} + q^{s-2} + \dots + 1 + q^{(s-1)/2} B(p^r + 1, s + 1)$$

of the previous section. While the Theorem (2.1) was established in [25], using character theory on the finite field, the Hermitian case is far simpler than the general diagonal case. Notice that for an arbitrary $\xi \in \mathbb{F}_q$, $\xi^{p^r+1} \in \mathbb{F}_{p^r}^*$. In other words the set of n -th roots of unity in \mathbb{F}_q are closed under addition, where $n = (q - 1)/(p^r + 1) = p^r - 1$ and are all the nonzero elements of \mathbb{F}_q^* . It follows that the quantity $N_{2,1,s}$ of the previous section is identically zero for all s .

Consider the set of solutions to the $(s + 1)$ dimensional Hermitian equation. These include The set of solutions to the s dimensional case with a zero added in the $(s + 1)$ -st position. In addition, any projective $(s + 1)$ -tuple that is not a solution to the s -dimensional case can be extended to $(p^r + 1)$ solutions to a projective $(s + 2)$ -tuple that is a solution to the $(s + 1)$ dimensional surface. This implies the size of the $(s + 1)$ dimensional Hermitian surface is:

$$(11) \quad h_{s+1} = (p^r + 1)(\pi_s - h_s) + h_s.$$

which is essentially Lemma (2.2) with $k = 1$, that is this recursion easily leads to the expression Equation (10). The three approaches above are equivalent. The last approach will be used in the remainder of the section.

The recursion equations of the previous section have an interesting implication on the recursive structure of the sets of solutions of the Hermitian equations. Let $\mathbb{P}^s = \mathbb{P}_q^s$, ($q = p^{2r}$)

be the set of projective $(s+1)$ -tuples over \mathbb{F}_q and $|\mathbb{P}^s| = \pi_s$ which for conformity we denote as p_s .

To discuss this recursive aspect of the Hermitian solutions sets, let P_s denote the $(s+1) \times p_s$ matrix with columns formed (in some order) from the elements of \mathbb{P}^s . Similarly denote by $\mathcal{H}_s \subset \mathbb{P}^s$ as the set of $(s+1)$ -tuples of the s -th order Hermitian variety, $h_s = |\mathcal{H}_s|$ and H_s the $(s+1) \times h_s$ matrix of these $(s+1)$ -tuples over \mathbb{F}_q . Further, denote by \mathcal{A}_s the difference $\mathbb{P}^s \setminus \mathcal{H}_s$ and let $a_s = p_s - h_s$ and A_s the $(s+1) \times a_s$ matrix of the corresponding $(s+1)$ -tuples.

Each $(s+1)$ -tuple in \mathcal{A}_s does not satisfy the s dimensional Hermitian equation Equation (9). Suppose $(a_0, a_1, \dots, a_s) \in \mathcal{A}_s$ then

$$a_0^{p^r+1} + a_1^{p^r+1} + \dots + a_s^{p^r+1} = b \in \mathbb{F}_{p^r}^*,$$

i.e. since each of the (p^r+1) -th powers of elements in \mathbb{F}_q is in $\mathbb{F}_{p^r}^*$ so is their sum (and this is a major difference between the Hermitian and general diagonal case where the sum may or may not be in U_n). Thus, in this case, each such $(s+1)$ -tuple in \mathcal{A}_s can be extended to $(p^r+1)(s+2)$ -tuples that are solutions to the $(s+1)$ dimensional case i.e. the equation $x_{s+1}^{p^r+1} = -b \in \mathbb{F}_{p^r}$ will have (p^r+1) solutions, say $b_1, b_1\eta, b_1\eta^2, \dots, b_1\eta^{p^r}$ where b_1 is chosen arbitrarily (but fixed) from the set and η is a (p^r+1) -th root of unity. Thus $(a_0, a_1, \dots, a_s) \in \mathcal{A}_s$ yields (p^r+1) solutions to the $(s+1)$ dimensional case of the form $(a_0, a_1, \dots, a_s, b_1^j)$ of \mathcal{A}_{s+1} .

Let $\mathbf{b} = (b_1, b_2, \dots, b_{a_s})$ and $\mathbf{b}_i = \eta^i \mathbf{b}$, $i = 0, 1, \dots, p^r$ where the b_i are representatives of the solutions. The discussion implies the form of the solutions of to the $(s+1)$ -dimensional case, (i.e. the elements of \mathcal{H}_{s+1}) in terms of the s -dimensional case and the corresponding matrices H_s and H_{s+1} , and reflecting the recursion of Equation (11), by appropriate permutations of the columns, can be viewed as:

$$H_{s+1} = \begin{array}{c|c|c|c|c|c} \mathbf{b} & \eta\mathbf{b} & \dots & \eta^{p^r}\mathbf{b} & 0 & 0 \dots 0 \\ \hline & & & & & x_{s+1} \\ & & & & & x_s \\ & & & & & \vdots \\ & & & & & x_1 \\ & & & & & x_0 \end{array}$$

FIGURE 1

The above observations have an implication for the structure of the evaluation code derived from Hermitian surfaces. An *evaluation code* [24, 23] for a variety X is given by the following map:

$$\begin{array}{ccc} \mathbb{F}_q[x_0, \dots, x_m]_h^\nu & \longrightarrow & \mathbb{F}_q^n \\ f & \mapsto & c(f) = (f(P_1), f(P_2), \dots, f(P_n)) \end{array}$$

where P_1, \dots, P_n are a subset of the rational points of the variety and f a homogeneous polynomial on the $(m+1)$ variables of degree h . When the set of points is the full set of rational points in \mathbb{P}^s , the set of rows generated by monomials of degree $\leq h$ acting on the $(s+1) \times p_s$ matrix, similar to the Hermitian one above, form the generator matrix of a code, called the s -th order projective geometry code over \mathbb{F}_q . The code is denoted by $C_P(h, s, q)$ and its parameters of dimension and minimum distance are well known [17, 18, 20, 21, 22].

Similarly, the code generated when the full set of points on the s dimensional Hermitian variety, is denoted by $C_H(h, s, q)$ and as noted this is a punctured subcode of $C_P(h, s, q)$. Considerably less is known about the Hermitian codes.

One of the original motivations for this work was to determine the recursive structure of the point sets, as above, and exploit this to determine properties of the Hermitian codes i.e. it had been hoped to determine properties of the code $C_H(h, s+1, q)$ in terms of those of $C_H(h, s, q)$ via the structure of the above matrix. This seems a difficult task and progress has been limited. Nonetheless the structure of the matrix is of independent interest in this regard.

It is noted [16] that for the case of $h = 1$ the code $C_H(1, s, q)$ has only two weights,

$$p^r(2s-1) + (-1)^{s-1}p^{s-1} \quad \text{and} \quad p^{r(2s-1)}.$$

This result is directly observable from the above matrix Equation 4.

A considerable effort has been made ([1, 2, 6, 7, 8, 10, 9, 12, 19]) to determine properties of the *quadric* Hermitian codes ($h = 2$) and it has been a challenging problem to determine information on the code. While some information on this case can be gleaned from the form of the matrix, one needs information on weights in the projective code and how they combine with weights of words in the Hermitian code for the case of $h = 2$ for a given monomial and the situation is more complex. A new approach to the problem would be of interest.

5. COMMENTS

Some aspects of the structure of the solution sets of multivariate diagonal equations over a finite field have been considered and the zeta functions of such an equation found explicitly, (which was already implicit in the work of Wolfmann [25]).

It is noted that Hermitian surfaces, where the degree of the equation depends on the size of the field of definition, does not have a zeta function. As a matter of interest define the Hermitian equation

$$x_0^{p^{kr+1}} + x_1^{p^{kr+1}} + \dots + x_s^{p^{kr+1}} = 0.$$

and seek solutions over \mathbb{F}_{q^k} , $q = p^{2r}$. Thus the degree of the Hermitian equation increases with the size of the extension field. One could define a 'zeta like' function by examining the enumeration as k increases. Let $N'_{k,s}$ denote the number of projective solutions to this equation over \mathbb{F}_{q^k} and note that:

$$\begin{aligned} N'_{k,s} &= (q^{ks} - 1)/(q - 1) + q^{k(s-1)/2} B(p^{rk} + 1, s + 1) \\ &= \begin{cases} \pi_{q^k, s-1} + p^{rks} \{ \sum_{j=0}^{a-1} p^{2jrk+1} - \sum_{j=0}^{a-1} p^{2rkj} \} & s = 2a, \\ \pi_{q^k, s-1} + p^{rks} \{ \sum_{j=0}^a p^{2jrk} - \sum_{j=0}^{a-1} p^{2rkj+1} \} & s = 2a + 1, \end{cases} \end{aligned}$$

Noting that

$$\sum_{k=1}^{\infty} p^{jrsk} t^k / k = -\ln(1 - p^{jrs} t)$$

define the polynomials

$$P(t) = \prod_{i=1}^{ks-1} (1 - q^i t), \quad P_1(t) = \prod_{i=0}^{a-1} (1 - p^{r(s+2j)} t).$$

With this definition the resulting ‘zeta function’ is:

$$Z(t) = \exp\left\{\sum_{k=1}^{\infty} N'_{k,s} t^k / k\right\} = \begin{cases} \frac{1}{P(t) \cdot P_1(t)^{p-1}}, & s = 2a \\ \frac{P_1(t)^{(p-1)}}{(1 - p^{r(s+2a)} t) \cdot P(t)}, & s = 2a + 1. \end{cases}$$

This is to be compared to the Theorem (3.2) with $d = p^r + 1$ where the diagonal equation degree is constant.

REFERENCES

- [1] Y. Aubry, Reed-Muller codes associated to projective algebraic varieties, Luminy Conference, *Lecture Notes in Mathematics*, No. 1518, 4–17, (1992).
- [2] D. Bartoli, M. De Boeck, S. Fanali and L. Storme, On the functional codes defined by quadrics and Hermitian varieties, *Designs, Codes and Cryptography*, **71**, no. 1, 21–46, (2014).
- [3] R.C. Bose and I.M. Chakravarti, Hermitian varieties in a finite projective space $PG(N, q)$, *Canad. J. Math.*, v. 18, 1161–1182 (1966).
- [4] R.C. Bose, On the application of finite projective geometry for deriving a certain series of balanced Kirkman arrangements, *Calcutta Math. Society*, 341–354, (1958–59).
- [5] R. Calderbank and W. Kantor, The geometry of two weight codes, *Bull. London Math. Soc.*, **18**, 97–122, (1986).
- [6] J.P. Cherdieu and R. Rolland, On the number of points of some hypersurfaces in \mathbb{F}_q^n , *Finite fields and their applications*, **2**, 214–224, (1996).
- [7] F. Edoukou, Codes defined by forms of degree 2 on Hermitian surfaces and Sørensen’s conjecture, *Finite fields and their applications*, **13**, 616–627, (2008).
- [8] F. Edoukou, S. Ling and C. Xing, Intersection of two quadrics with no common hyperplane in $\mathbb{P}^n(\mathbb{F}_q)$, arXiv:0907.4556v1.
- [9] F. Edoukou, A. Hallex, F. Rodier and L. Storme, The small weight codewords of the functional codes associated to non-singular Hermitian varieties, *Designs, Codes and Cryptography*, **56**, 219–233, (2010).
- [10] F. Edoukou, S. Ling and C. Zing, Structure of functional codes defined on non-degenerate Hermitian varieties, *J. Combinatorial Theory, Ser. A*, **118**, 2436–2444, (2011).
- [11] S.R. Ghorpade and G. Lachaud, Number of solutions of equations over finite fields and a conjecture of Lang and Weil, *Trends in Mathematics*, Birkhäuser, Basel, 269–291, (2002).
- [12] A. Hallez and L. Storme, Functional codes arising from quadric intersections with Hermitian varieties, *Finite fields and their applications*, **16**, 27–35, (2010).
- [13] S.H. Hansen, Error-correcting codes from higher dimensional varieties, *Finite fields and their applications*, **7**, 530–552, (2001).

- [14] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, GTM vol. 84, 2nd. edition, Springer-Verlag, New York, (1990).
- [15] N. Koblitz, *p-adic Numbers, p-adic analysis and zeta functions*, Springer-Verlag, New York, (1977).
- [16] J.B. Little, Algebraic geometry codes from higher dimensional varieties, *Advances in algebraic geometry codes*, 257-293, Ser. Coding Theory Cryptol., **5**, World Sci. Publ., Hackensack, NJ, (2008).
- [17] G. Lachaud, Number of points of plane sections and linear codes defined on algebraic varieties, in *Arithmetic, Geometry and Coding Theory*, Proceedings of Luminy Conference, Walter de Gruyter (1993).
- [18] G. Lachaud, The parameters of projective Reed-Müller codes, *Discrete Mathematics*, **81**, 217–221, (1990).
- [19] A. Sboui, Second highest number of points of hypersurfaces in \mathbb{F}_q^n , *Finite fields and their applications*, **13**, 444-449, (2007).
- [20] Anders B. Sørensen, Projective Reed-Müller codes, *IEEE Transactions on Information Theory*, **17**, 1567–1576, (1991).
- [21] Anders B. Sørensen, *Rational points on hypersurfaces, Reed-Muller codes and algebraic geometric codes*, Ph.D. Thesis, Aarhus, November, (1991).
- [22] Anders B. Sørensen, On the number of rational points on codimension-1 algebraic sets in $\mathbb{P}^n(\mathbb{F}_q)$, *Discrete Math.*, **135**, 321–324, (1994).
- [23] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, New York, (1991).
- [24] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic geometric codes: Basic notions*, Mathematical Surveys and Monographs, AMS vol. 139, (2007).
- [25] J. Wolfmann, The number of solutions of certain diagonal equations over finite fields, *J. Number Theory*, **42**, 24–257, (1992).
- [26] K. Yang and V. Kumar, On the true minimum distance of Hermitian codes, *Lecture Notes in Mathematics*, Springer-Verlag, **1518**, 99–107, (1992).
- [27] M. Zarzar, Error-correcting codes on low rank surfaces, *Finite Fields and their Applications*, **13**, 727–737, (2007).

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING, UNIVERSITY OF BRITISH COLUMBIA,
VANCOUVER, BC, V6T 1Z4

E-mail address: ifblake@ece.ubc.ca

DEPARTMENT OF MATHEMATICS. UNIVERSITY OF TORONTO, TORONTO, ON M5S 2E4

E-mail address: murty@math.toronto.edu

DEPARTMENT OF MATHEMATICS, MEMORIAL UNIVERSITY, ST. JOHN'S, NL, A1C 5S7

E-mail address: usefi@mun.ca